

REMARKS/ARGUMENTS

This Amendment is in response to the Final Office Action of August 9, 2005, in which the Examiner rejected all pending claims (claims 1-21). Claims 1-5 and 9-21 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,365,591 ("**Carswell**") in view of U.S. Patent No. 5,892,904 ("**Atkinson**"), and claims 6-8 were rejected under 35 U.S.C. 103(a) as being unpatentable over **Carswell** in view of **Atkinson** and in further view of **Office Notice**.

By the present amendment, claims 1 and 15 have been amended and claim 22 has been added. After entry, claims 1 through 22 would be pending.

Applicant's invention, as explained in the specification, is a method and system for authenticating messages in a dual processor device. The invention uses a host processor and a secure processor, with the dual processor device receiving an encrypted message and passing the message (in decrypted form) to the host processor if the message is authenticated by the secure processor. Thus, in order to avoid the host processor being hacked or reprogrammed to skip the authentication process, the decrypted message is not passed to the host processor unless it is authenticated by the secure processor.

Applicant has amended claim 1 (and claim 15) to clarify the claimed subject matter, without adding new matter or changing the scope thereof. Thus, for example, in claim 1, there is now included the additional language (believed by Applicant to be implicit in the claim as originally presented) that "if the message is not authentic, not transferring the decrypted message to the host processor."

Applicant respectfully submits that the cited references, **Carswell** and **Atkinson**, do not teach, show or suggest the present invention, either individually or as combined by the Examiner.

Carswell discloses a multi-processor device including a crypto processor 30 and a number of other processors, including a red processor 20 for receiving/providing plain text (unencrypted messages) to the crypto processor and black processor 40 for receiving/providing cipher text (encrypted messages) to the crypto processor (e.g., see col. 1, line 55 and col. 3, lines

13-32). In **Carswell**, the crypto processor 30 encrypts/decrypts messages. Unlike, the present invention, there is no "host processor" that receives a decrypted message only "if said message is authentic" as determined by the secure processor.

Atkinson discloses sending files with certificates to insure authenticity and integrity (see Abstract; col. 2, lines 34-37). It likewise does not disclose a host processor and a secure processor where encrypted messages are transferred to the host processor only "if said message is authentic", as recited in claim 1.

Carswell and **Atkinson** do not teach Applicant's invention, even if combined, since neither shows a host processor and a secure processor having the features as recited in claim 1. If combined, they would show at most encrypted messages having authentication certificates, with all encrypted messages provided (through a "black processor") to a single "crypto processor", and all unencrypted messages provided (through a red processor) to a crypto processor. This is clearly different from Applicant's claimed invention having a secure processor that authenticates and decrypts messages, and a host processor to which the decrypted messages are transferred if authenticated by the secure processor (and not transferred if they are not authentic).

Applicant notes the Examiner's apparent belief that the red processor 20 of **Carswell** is the same as Applicant's host processor (see paragraph 13 of the Remarks). Applicant respectfully disagrees. The most analogous component in **Carswell** to Applicant's host processor is the computer 10 (Fig.1). The link encryptor 11 (including crypt processor 30 and red processor 20, and black processor 40) is analogous to the Applicant's secure processor and is responsible for encrypting plain text data received from computer 10 and decrypting encrypted text data (from modem 12) for transfer to computer 10 (see col. 2, lines 42-58). The red and black processors in **Carswell** receive all messages, since the purpose of each is to act as a processing conduit (all plain text messages from computer 10 are passed by red processor 20 to crypto processor 30 for encryption and all encrypted messages from modem 12 are passed by black processor 40 to crypto processor 30 for decryption). Thus, red processor 20 is not a host processor, but merely a path for passing all plain text (unencrypted) data from computer 10 to

Appl. No. 09/890,179
Amdt. dated October 7, 2005
Amendment under 37 CFR 1.116 Expedited Procedure
Examining Group 2134

PATENT

crypto processor 30, rather than a host processor that receives only decrypted messages that have been authenticated, as recited in claim 1.

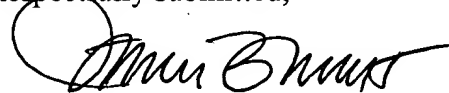
System claim 15 and new claim 22 are similar to claim 1, and are believed allowable for the same reasons, as are dependent claims 2-14 and 16-21.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.

Respectfully submitted,



Stephen F. Jewett
Reg. No. 27,565

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 415-576-0300
SFJ:bhr
60603903 v1